AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of the claims in the application:

1. (Currently amended) In a computer-implemented ~~trust~~ authorization management system, a method for controlling a user's access to a computing resource that is managed by said computer-implemented authorization management system, the method including:

~~obtaining~~ receiving an electronic request for the computing resource;

~~obtaining~~ retrieving a group of computer-readable authorization certificates from at least one computer-readable authorization certificate storage location accessible to said computer-implemented authorization management system, each certificate ~~expressing~~ containing at least one computer-readable authorization by at least one principal;

identifying a set of principals associated with the computer-readable authorization certificates;

~~initializing~~ creating a lattice of authorization values ~~state~~ associated with each principal of said set of principals in a memory device in communication with the computer-implemented authorization system, wherein said authorization values are a monotone function of the authorizations of the set of principals;

evaluating a certificate as a monotone function, at least in part, of the authorization value ~~state~~ associated with one or more of the principals;

updating the authorization value ~~state~~ of one or more of the principals if the result of said evaluating step indicates that the authorization value ~~state~~ of a principal should be changed; and

repeating said evaluating and updating steps until a fixpoint of said lattice of authorizations values is reached ~~or until a predefined principal is found to authorize the request~~.

2. (Currently amended) A method as in claim 1, further including:

constructing a dependency graph representation in a memory device in communication with the computer-implemented authorization system, the dependency graph containing a node corresponding to each principal in the set of principals; and

~~connecting~~ assigning at least two nodes in the dependency graph with a certificate that expresses a dependency of one node on the state of another node;

wherein the dependency graph representation is used, at least in part, during said evaluating, updating, and repeating ~~steps~~ to determine which certificates to evaluate.

3. (Currently amended) A method as in claim 1, in which said updating ~~step~~ is performed after all of the certificates have been evaluated.

4. (Currently amended) A method as in claim 1, in which the request for the computing resource is ~~obtained~~ received from a first principal, and in which at least one of the certificates is ~~obtained~~ received from the first principal, the certificate having been issued by a second principal.

5. (Original) A method as in claim 1, in which the certificates comprise Simple Public Key Infrastructure certificates.

6. (Currently amended) A method as in claim 1, in which the ~~computing resource~~ request is to ~~one of~~: access to a piece of electronic content; use ~~of~~ a computer program; ~~ability to~~ execute a transaction; access ~~to~~ a computer; ~~and~~ or access ~~to~~ a network.

7. (Currently amended) A computer program product for making ~~trust~~ authorization management determinations for controlling a user's access to a computing resource that is managed by said computer-implemented authorization management system, the computer program product including:

computer code for ~~obtaining~~ receiving an electronic request to perform a predefined action;

computer code for ~~obtaining~~ retrieving a group of computer-readable authorizations for the predefined action from at least one computer-readable authorization certificate storage location accessible to said computer-implemented authorization management system, one or more of the authorizations in the group being a monotone function of the authorization state of one or more principals;

computer code for identifying a set of principals associated with the authorizations and for initializing ~~a state~~ a lattice of authorization values associated with each principal of said set of principals in a memory device in communication with the computer-implemented authorization system;

computer code for evaluating authorizations from the set of authorizations using the authorization value ~~state~~ associated with each principal;

computer code for updating the authorization value ~~state~~ of the principals;

computer code for causing repeated execution of said computer code for evaluating authorizations and for updating the authorization value ~~state~~ of the principals until a fixpoint of said lattice of authorization values is reached ~~or until a predefined principal is deemed to authorize the request~~; and

a computer-readable medium for storing the computer codes.

8. (Currently amended) A computer program product as in claim 7, in which the computer-readable medium is one of: CD-ROM, DVD, MINIDISC, floppy disk, magnetic tape, flash memory, ROM, RAM, system memory, network server, hard drive, and optical storage~~, and a data signal embodied in a carrier wave~~.

9. (Currently amended) A computer-implemented system for controlling access to electronic content or processing resources managed by a computer-implemented authorization management system, the system comprising:

means for receiving [[a]] an electronic request from a requesting principal to access a piece of electronic content or a processing resource;

means for collecting a set of one or more computer-readable authorization certificates relating to the request, the requesting principal, or the electronic content or processing resource from at least one computer-readable authorization certificate storage location accessible to said computer-implemented authorization management system;

means for identifying a root principal from whom authorization is needed in order to grant the request;

means for creating a lattice of monotone authorization values in a memory device associated with in a memory device in communication with said system and performing at least a portion of a least fixpoint computation over said authorization values to determine whether the root principal has authorized the

requesting principal to access the piece of electronic content or processing resource; and

means for granting the requesting principal access to the electronic content or processing resource ~~if~~ when the least fixpoint computation indicates that the root principal has authorized said access.

10. (Currently amended) A computer-implemented system for controlling access to computer-controlled electronic resources, the system comprising:

a first computer system for processing electronic requests for access to computer-controlled electronic ~~system~~ resources, the first computer system comprising:

a computer network interface ~~for receiving~~ configured to receive digital certificates from other computer systems and for electronically receiving and processing requests to access electronic resources;

a memory device in communication with said first computer system for storing electronic resources and one or more computer-readable authorization certificates relating to authorization for controlling access thereto; and

a trust management engine for processing digital certificates and requests for electronic resources, and for making access control decisions by

creating a lattice of monotone authorization values in a memory device associated with in a memory device in communication with said system and performing least fixpoint computations using said authorization values ~~digital certificates~~.

11. (Currently amended) A system as in claim 10, further comprising:

a second computer system for making a request for system resources from the first computer system; and

a third computer system for generating a first digital certificate, the first digital certificate including an authorization value that is generated from a monotone function, the authorization value effective for authorizing, at least in part, the second computer system to access a predefined system resource.

12. (Currently amended) A system as in claim 11, further comprising:

a fourth computer system, the fourth computer system being operable to generate a second digital certificate including an authorization value that is generated from a monotone function, the second digital certificate authorizing, at least in part, the third computer system to authorize, at least in part, the user of the second computer system to access the predefined system resource.

13. (Currently amended) A system as in claim 12, in which the third computer system is operable to ~~send~~ transmit the first digital certificate to the second computer system, the second computer system is operable to ~~send~~ transmit the first digital certificate to the first computer system in connection with said request, and the fourth computer system is operable to ~~send~~ transmit the second digital certificate to the first computer system.

14. (Currently amended) A system as in claim 13, in which the first computer system further comprises a public key stored in a memory device in communication with said first computer system and associated with the fourth computer system, the public key corresponding to a private key used to sign the second digital certificate.

15. (Original) A system as in claim 10, in which at least some of the digital certificates comprise SPKI certificates.

16. (Original) A system as in claim 10, in which at least some of the digital certificates comprise Keynote certificates.

17. (Currently amended) A computer-implemented method for performing ~~trust~~ authorization management computations using a computer system, the method including:

~~collecting~~ receiving a group of computer-readable certificates stored in a memory device in communication with said computer system, each certificate including at least one authorization value;

~~expressing authorizations~~ defining said authorizations values in said certificates using monotone authorization values ~~a structure that satisfies certain predefined properties~~;

~~expressing each certificate as a function, wherein each function possesses one or more properties sufficient to ensure that a set of authorizations will have a fixpoint~~ creating a lattice of said authorization values in the memory device in communication with said computer system; and

computing a fixpoint ~~of the authorizations~~, or an approximation thereof, from said lattice;

~~making a trust~~ to make thereby an authorization management decision.

18.–20. (Canceled)